Dell™ AppAssure™ 5.4.3

Guia de integração de terceiros

© 2014 Dell Inc.
TODOS OS DIREITOS RESERVADOS.

Este guia contém informações proprietárias protegidas por direitos autorais. O software descrito neste guia é fornecido com uma licença de software ou um acordo de não divulgação. Este software pode ser usado ou copiado somente segundo os termos do acordo aplicável. Nenhuma parte deste guia pode ser reproduzida ou transmitida de qualquer forma ou por qualquer meio, eletrônico ou mecânico, incluindo fotocópias e gravações para qualquer outro fim que não o uso pessoal do comprador sem permissão por escrito da Dell Inc.

As informações contidas neste documento são fornecidas em conjunto com os produtos da Dell. Nenhuma licença, expressa ou implícita, por preclusão ou de outra forma, a quaisquer direitos de propriedade intelectual é concedida por este documento ou em conexão com a venda dos produtos da Dell. EXCETO CONFORME DEFINIDO NOS TERMOS E CONDIÇÕES ESPECIFICADOS NO ACORDO DE LICENÇA DESTE PRODUTO, A DELL NÃO ASSUME NENHUMA RESPONSABILIDADE E RENUNCIA QUALQUER GARANTIA EXPRESSA, IMPLÍCITA OU ESTABELECIDA POR LEI RELACIONADA A SEUS PRODUTOS INCLUINDO, MAS NÃO LIMITADO A, GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA OU NÃO VIOLAÇÃO. EM NENHUMA CIRCUNSTÂNCIA A DELL SERÁ RESPONSÁVEL POR QUAISQUER DANOS DIRETOS, INDIRETOS, CONSEQUENCIAIS, PUNITIVOS, ESPECIAIS OU INCIDENTAIS (INCLUINDO, SEM LIMITAÇÃO, DANOS POR PERDA DE LUCROS, INTERRUPÇÃO DE NEGÓCIOS OU PERDA DE INFORMAÇÕES) RESULTANTES DO USO OU DA INCAPACIDADE DE USAR ESTE DOCUMENTO, MESMO SE A DELL TIVER SIDO NOTIFICADA A RESPEITO DA POSSIBILIDADE DE TAIS DANOS. A Dell não faz representações ou garantias com relação à precisão ou integridade do conteúdo deste documento e se reserva o direito de fazer alterações em especificações e descrições de produtos a qualquer momento e sem aviso. A Dell não faz nenhum compromisso em atualizar as informações contidas neste documento.

Se você tem quaisquer dúvidas ou perguntas sobre seu potencial uso deste material, entre em contato com:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Consulte o nosso website (software.dell.com) para obter informações de contato de escritórios regionais e internacionais.

Marcas registradas

Dell, o logotipo da Dell e AppAssure são marcas registradas da Dell Inc. e/ou seus afiliados. Outras marcas registradas e nomes comerciais poderão ser usados neste documento para se referir às entidades proprietárias das marcas e nomes ou a seus produtos. A Dell renuncia qualquer interesse de propriedade nas marcas e nomes de terceiros.

Legendas

CUIDADO: o ícone de CUIDADO indica a possibilidade de danos ao hardware ou perda de dados caso as instruções não sejam seguidas.

AVISO: o ícone de AVISO indica a possibilidade de danos à propriedade, ferimentos pessoais ou morte.

NOTA IMPORTANTE, **NOTA**, **DICA**, **MÓVEL** ou **VÍDEO:** o ícone de informações indica uma informação extra/de apoio.

Dell AppAssure
Guia de integração de terceiros
Atualizado - Dezembro de 2014
Versão de software - 5.4.3

Conteúdo

Introdução ao AppAssure 4
Principais tecnologias do AppAssure 5
Live Recovery 5
Verified Recovery 5
Universal Recovery 5
True Global Deduplication 5
Arquitetura True Scale do AppAssure 6
Arquitetura de implementação do AppAssure 7
Recursos do produto do AppAssure 10

Instalação e configuração do AppAssure Add-on for Kaseya e do software do AppAssure 18
Preparar o AppAssure Add-on for Kaseya 18
Instalação do AppAssure Add-on for Kaseya 19
Desinstalação do AppAssure Add-on for Kaseya 19
Requisitos do sistema do AppAssure 20
Gerenciamento de suas licenças do AppAssure 23
Instalação do AppAssure usando o Kaseya 24

Uso do AppAssure Add-on for Kaseya 28
Gerenciamento de credenciais do AppAssure Core e do agente 28
Configuração de repositórios 30
Configuração da proteção de máquina 33
Gerenciamento da replicação 34
Monitoramento da atividade do AppAssure 37
Gerenciamento de relatórios do AppAssure Core 38

Sobre a Dell 40
Contatos da Dell 40
Recursos do suporte técnico 40

1

Introdução ao AppAssure

Este capítulo fornece uma introdução e uma visão geral do AppAssure. Ele descreve os recursos, a funcionalidade e a arquitetura, e consiste nos seguintes tópicos:

- Principais tecnologias do AppAssure
- Arquitetura True Scale do AppAssure
- Arquitetura de implementação do AppAssure
- Recursos do produto do AppAssure

O AppAssure estabelece um novo padrão de proteção de dados unificada, combinando backup, replicação e recuperação em uma única solução, projetada para ser o backup mais rápido e confiável para a proteção de máquinas virtuais (VM), ambientes físicos e de nuvem.

O AppAssure combina backup e replicação em um produto de proteção de dados integrada e unificada, que também fornece reconhecimento do aplicativo para garantir uma recuperação confiável de dados de aplicativo a partir dos backups. O AppAssure se baseia na nova arquitetura True Scale™ (patente pendente), que proporciona o desempenho de cópia de segurança mais rápido com objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO) muito agressivos, próximos de zero.

O AppAssure combina várias tecnologias exclusivas, inovadoras e avançadas:

- Live Recovery
- Verified Recovery
- Universal Recovery
- True Global Deduplication

Essas tecnologias são projetadas com integração segura para a recuperação após desastres na nuvem e proporcionam uma recuperação rápida e confiável. Com seu armazenamento escalável de objetos, o AppAssure tem uma capacidade exclusiva de processar petabytes de dados muito rapidamente, com eliminação da duplicação de dados global embutida, compactação, criptografia e replicação para qualquer infraestrutura de nuvem pública ou privada. Aplicativos e dados de servidor podem ser recuperados em minutos, para fins de retenção de dados e conformidade.

As ferramentas de cópia de segurança legadas atuais e as ferramentas de cópia de segurança com VM da primeira geração são ineficientes e ineficazes. As ferramentas de cópia de segurança desatualizadas não têm capacidade de trabalhar com dados em grande escala e não oferecem o nível de desempenho e confiabilidade necessário para proteger aplicativos críticos para os negócios. A combinação dessas características com ambientes de TI complexos e mistos representa um desafio administrativo para os profissionais de TI e vulnerabilidades para os dados do sistema.

O AppAssure enfrenta essa complexidade e ineficiência com a nossa tecnologia de core e suporte de ambientes com vários hypervisors, incluindo os que executam em VMware vSphere e Microsoft Hyper-V, que englobam nuvens públicas e privadas. O AppAssure oferece esses avanços tecnológicos e, ao mesmo tempo, reduz drasticamente os custos de gerenciamento de TI e armazenamento.

Principais tecnologias do AppAssure

Detalhes sobre as principais tecnologias do AppAssure são descritos nos tópicos a seguir.

Live Recovery

Live Recovery é uma tecnologia de recuperação instantânea para VMs ou servidores. Oferece acesso quase contínuo a volumes de dados em servidores virtuais ou físicos. É possível recuperar um volume inteiro com RTO próximo de zero e RPO de minutos.

A tecnologia de cópia de segurança e replicação do AppAssure registra snapshots simultâneos de várias VMs ou servidores, proporcionando proteção quase instantânea de dados e do sistema. É possível retomar o uso do servidor diretamente do arquivo de cópia de segurança, sem esperar uma restauração completa para o armazenamento de produção. Os usuários mantêm a produtividade e os departamentos de TI reduzem as janelas de recuperação para cumprir os contratos de nível de serviço atuais de RTO e RPO, cada vez mais exigentes.

Verified Recovery

O Verified Recovery permite realizar testes de recuperação e confirmação de cópias de segurança de forma automatizada. Ele inclui, entre outros, os sistemas de arquivo: Microsoft Exchange Server 2007, 2010 e 2013; e Microsoft SQL Server 2005, 2008, 2008 R2, 2012 e 2014. O Verified Recovery fornece capacidade de recuperação de aplicativos e cópias de segurança em ambientes físicos e virtuais. Ele também oferece um algoritmo abrangente de verificação de integridade, baseado em chaves de SHA de 256 bits que verificam a correção de cada bloco do disco na cópia de segurança durante as operações de arquivamento, replicação e propagação de dados. Essa capacidade garante a identificação precoce da corrupção de dados e impede que os blocos de dados corrompidos sejam mantidos ou transferidos durante o processo de cópia de segurança.

Universal Recovery

A tecnologia Universal Recovery oferece uma flexibilidade ilimitada de restauração de máquina. É possível restaurar suas cópias de segurança de um meio físico para virtual, de virtual para virtual, de virtual para físico ou de físico para físico. Também é possível realizar bare metal restores para hardware distinto; por exemplo, P2V, V2V, V2P, P2P, P2C, V2C, C2P e C2V.

Também acelera as movimentações entre plataformas entre as máquinas virtuais, por exemplo: mover de VMware para Hyper-V ou de Hyper-V para VMware. Baseia-se na recuperação no nível de aplicativo, nível do item e nível do objeto: arquivos individuais, pastas, e-mail, itens de calendário, bancos de dados e aplicativos. Com o AppAssure, também é possível recuperar ou exportar de físico para a nuvem ou do virtual para a nuvem.

True Global Deduplication

O AppAssure fornece a true global deduplication, que reduz drasticamente os requisitos de capacidade do disco físico, oferecendo taxas de redução de espaço que passam de 50:1 e, mesmo assim, atendem aos requisitos de armazenamento de dados. A compressão embutida no nível do bloco da arquitetura True Scale e a deduplicação com desempenho com velocidade de linha, juntamente com a verificação de integridade embutida, impede que a corrupção dos dados afete a qualidade dos processos de cópia de segurança e arquivamento.

Arquitetura True Scale do AppAssure

O AppAssure foi desenvolvido com a arquitetura True Scale do AppAssure. Utiliza uma arquitetura dinâmica, de pipeline e de vários cores otimizada para proporcionar consistentemente um desempenho com velocidade de linha para ambientes corporativos. A arquitetura True Scale é projetada de forma ascendente para escalar linearmente e armazenar e gerenciar big data eficientemente e fornecer RTOs e RPOs de minutos sem comprometer o desempenho. Inclui um gerenciador de objeto e volume feito sob medida com deduplicação global, compressão, criptografia, replicação e retenção integradas. O diagrama a seguir descreve a arquitetura True Scale do AppAssure.

Figura 1. Arquitetura True Scale do AppAssure

O AppAssure Volume Manager e o armazenamento escalável de objetos atuam como a base da arquitetura True Scale do AppAssure. O armazenamento escalável de objetos armazena snapshots no nível do bloco que são capturados a partir de servidores virtuais e físicos. O gerenciador de volume gerencia os vários armazenamentos de objetos, fornecendo um repositório comum ou armazenamento just-in-time somente para o que é necessário. O armazenamento de objetos suporta tudo simultaneamente com I/O assíncrona, que proporciona alta taxa de transferência com latência mínima e maximiza a utilização do sistema. O repositório reside em tecnologias de armazenamento diferentes, como rede de área de armazenamento (SAN), armazenamento por conexão direta (DAS) ou armazenamento conectado à rede (NAS).

A função do AppAssure Volume Manager é similar à do gerenciador de volume em um sistema operacional. Ela seleciona vários dispositivos de armazenamento, que podem ser de diversos tipos e tamanhos, e os combina em volumes lógicos, usando políticas de alocação distribuídas ou sequenciais. O armazenamento de objetos salva, recupera, mantém e, em seguida, replica objetos derivados de snapshots que reconhecem os aplicativos. O gerenciador de volume proporciona um desempenho de I/O escalável em conjunto com deduplicação global de dados, criptografia e gerenciamento de retenção.

Arquitetura de implementação do AppAssure

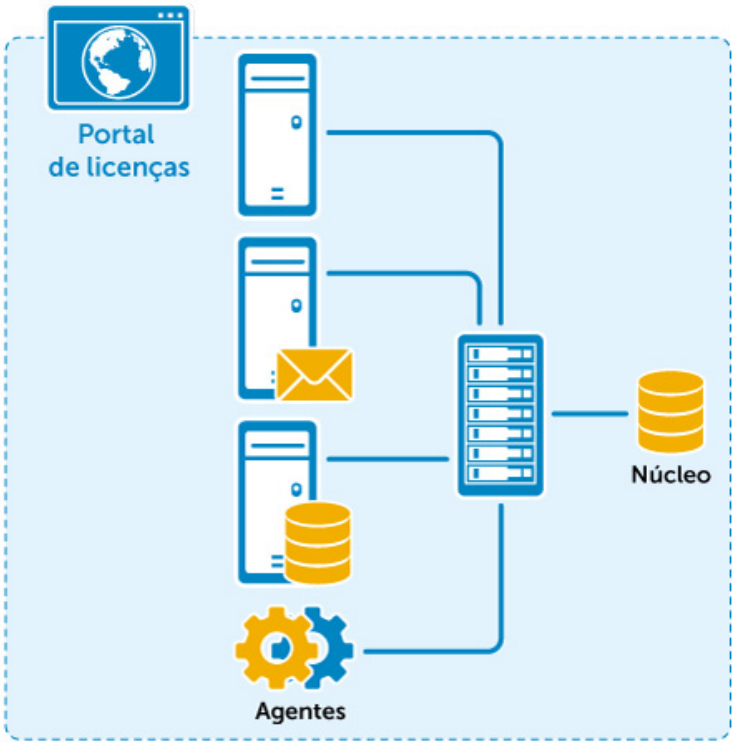
O AppAssure é um produto escalável de backup e recuperação, implementado de forma flexível na empresa ou como um serviço prestado por um provedor de serviços gerenciados. O tipo de implementação depende do tamanho e dos requisitos do cliente. A preparação para implementar o AppAssure envolve o planejamento da topologia de armazenamento na rede, hardware do core e infraestrutura de recuperação após desastres e segurança.

A arquitetura de implementação do AppAssure consiste em componentes locais e remotos. Os componentes remotos podem ser opcionais para as pessoas que não querem usar um site de recuperação após desastres ou um provedor de serviços gerenciados para a recuperação fora do local. Uma implementação local básica consiste em um servidor de cópia de segurança chamado de Core e uma ou mais máquinas protegidas, conhecida como Agent. O componente fora do local é ativado usando a replicação que fornece recursos completos de recuperação no site de DR. O AppAssure Core usa imagens de base e snapshots incrementais para compilar pontos de recuperação de agentes protegidos.

Além disso, o AppAssure reconhece o aplicativo, pois tem a capacidade de detectar a presença do Microsoft Exchange, do SQL e seus respectivos bancos de dados e arquivos de log e, em seguida, agrupa esses volumes automaticamente com dependência, para uma proteção abrangente e uma recuperação efetiva. Isso impede que haja cópias de segurança incompletas quando você realizar recuperações. As cópias de segurança são realizadas usando snapshots no nível do bloco que reconhecem o aplicativo. O AppAssure também pode realizar o truncamento de log dos servidores protegidos do Microsoft Exchange e do SQL.

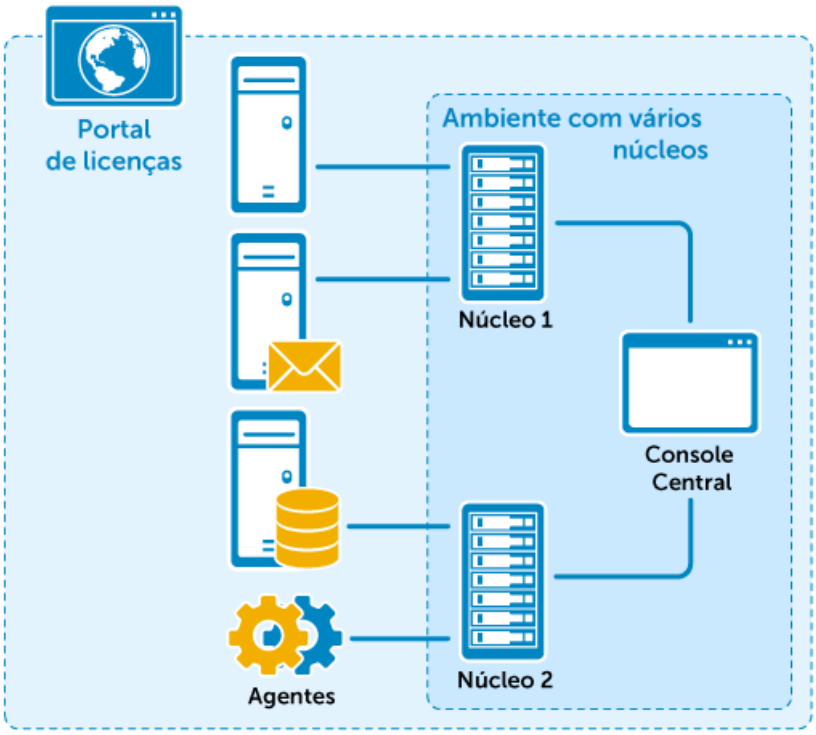
O diagrama a seguir descreve uma implementação simples do AppAssure. Nesse diagrama, os AppAssure Agents são instalados em máquinas, como um servidor de arquivos, de e-mail ou de banco de dados, ou em máquinas virtuais, conectam-se a um único AppAssure Core, que também é constituído pelo repositório central, e são protegidos por ele. O Portal de licenças do Dell AppAssure gerencia as assinaturas de licença, grupos e usuários para os agentes e cores do ambiente. Os usuários efetuam login no Portal de licenças para ativar contas, baixar o software e implementar agentes e cores de acordo com a licença para o seu ambiente.

Figura 2. Arquitetura de implementação do AppAssure



Também é possível implementar vários AppAssure Cores, conforme exibido no diagrama a seguir. Um console central baseado na Web gerencia vários cores.

Figura 3. Arquitetura de implementação de vários Cores do AppAssure



AppAssure Smart Agent

O AppAssure Smart Agent é instalado nas máquinas que serão protegidas pelo AppAssure Core. O Smart Agent rastreia os blocos alterados no volume de disco e, em seguida, cria um snapshot de uma imagem dos blocos alterados em um intervalo de proteção predefinido. A abordagem "para sempre" desses snapshots incrementais no nível do bloco impede a repetição da cópia dos mesmos dados da máquina protegida para o Core. O Smart Agent reconhece o aplicativo e fica inativo quando não está em uso, com quase zero por cento (0%) de utilização da CPU e menos de 20 MB de sobrecarga de memória. Quando o Smart Agent está ativo, ele chega a dois (2%) a quatro por cento (4%) de utilização da CPU e menos de 150 MB de memória, que inclui a transferência dos snapshots para o Core. Esse valor é muito inferior ao dos programas de software legados tradicionais, que usam níveis muito mais altos de CPU e largura de banda da memória, mesmo estando inativos.

O AppAssure Smart Agent reconhece os aplicativos porque detecta não somente o tipo de aplicativo instalado, mas também a localização dos dados. Ele agrupa automaticamente os volumes de dados com dependência como os bancos de dados e, em seguida, registra-os juntos para uma proteção efetiva e recuperação rápida. Após a configuração do agente, ele usa a tecnologia inteligente para acompanhar os blocos alterados nos volumes de disco protegidos. Quando o snapshot está pronto, ele é transferido rapidamente para o AppAssure Core usando conexões inteligentes, de multiprocessamento e baseadas em soquetes. Para preservar a largura de banda da CPU e a memória nas máquinas protegidas, o Smart Agent não criptografa nem faz a deduplicação dos dados na origem, e as máquinas do agente são pareadas com um core para proteção.

AppAssure Core

O AppAssure Core é o componente central da AppAssure arquitetura de implementação. O Core armazena e gerencia todas as cópias de segurança da máquina e presta serviços essenciais de cópia de segurança, de recuperação e retenção, bem como de replicação, arquivamento e gerenciamento. O Core é um servidor dedicado independente endereçável na rede que executa uma variante de 64 bits do sistema operacional Microsoft Windows. O AppAssure realiza compactação embutida, criptografia e deduplicação de dados baseada no destino dos dados recebidos a partir de um agente.

Em seguida, o Core armazena as cópias de segurança de snapshot em um repositório, que pode residir em diversas tecnologias de armazenamento, como rede de área de armazenamento (SAN), armazenamento com conexão direta (DAS) ou armazenamento conectado à rede (NAS). O repositório também pode residir em volumes de armazenamento interno no servidor Core. O Core é gerenciado acessando a seguinte URL em um navegador da Web habilitado para JavaScript: https://CORENAME:8006/apprecovery/admin. Internamente, todos os serviços do core podem ser acessados por meio das APIs (Application Programming Interfaces) REST (Representational State Transfer). Os principais serviços podem ser acessados de dentro do Core ou diretamente pela Internet, a partir de qualquer aplicativo que possa enviar uma solicitação de HTTP/HTTPS e receber uma resposta de HTTP/HTTPS. Todas as operações de API são realizadas em SSL e autenticadas mutuamente por meio de certificados X.509 v3.

Processo de snapshots

O processo de proteção do AppAssure começa quando uma imagem de base é transferida de uma máquina agente para o Core, seguida de snapshots incrementais para sempre. O software AppAssure Agent para Windows usa o Microsoft Volume Shadow Copy Service (VSS) para congelar e desativar os dados de aplicativo no disco a fim de capturar uma cópia de segurança consistente com o sistema de arquivos e com os aplicativos. Quando se cria um snapshot, o gravador do VSS no servidor de destino impede a gravação de conteúdo no disco. Durante o processo de impedir a gravação de conteúdo no disco, todas as operações de I/O no disco entram na fila e são retomadas somente depois que o snapshot é concluído; as operações ainda em andamento, por sua vez, serão concluídas e todos os arquivos abertos serão fechados. O processo de criar uma cópia de sombra não afeta muito o desempenho do sistema de produção.

O AppAssure usa o VSS da Microsoft porque ele tem suporte incorporado para todas as tecnologias internas do Windows, como NTFS, Registro, Active Directory, etc., para liberar dados para o disco antes do snapshot. Além disso, outros aplicativos corporativos, como o Microsoft Exchange e o SQL Server, usam plug-ins do VSS Writer para receber notificações quando um snapshot está sendo preparado e quando é necessário liberar as páginas de banco de dados usadas para o disco para que o banco de dados fique em um estado transacional consistente. É importante ressaltar que o VSS é usado para desativar os dados de sistema e aplicativo no disco; não é usado para criar o snapshot. Os dados capturados são transferidos rapidamente para o AppAssure Core e armazenados nele. O uso do VSS para a cópia de segurança não deixa o servidor de aplicativos no modo de cópia de segurança por um período longo, já que o tempo necessário para realizar o snapshot é medido em segundos e não em horas. Outro benefício do uso do VSS para cópias de segurança é o fato de ele permitir que uma máquina protegida obtenha um snapshot de grandes quantidades de dados simultaneamente, já que o snapshot funciona no nível do volume.

Replicação – Site de recuperação após desastres ou provedor de serviços

O processo de replicação no AppAssure requer um relacionamento pareado de origem/destino entre dois ou mais cores. Esse core de origem copia os pontos de recuperação de máquinas protegidas selecionadas e então transmite de modo assíncrono e contínuo os dados de snapshot incrementais para o core de destino em um site de recuperação após desastres remoto. O lugar externo pode ser um data center de propriedade da empresa (core autogerenciado), um local de terceiros de um provedor de serviços gerenciados (MSP) ou um ambiente de nuvem. Ao replicar para um core de destino de terceiros, é possível usar fluxos de trabalho incorporados que permitam solicitar conexões e receber notificações automáticas de feedback. Para a transferência inicial de

dados, é possível realizar a propagação de dados usando mídias externas; isso é útil para grandes conjuntos de dados ou sites com links lentos.

No caso de uma interrupção grave, o AppAssure suporta a ativação e a reativação pós-falha em ambientes replicados. Em caso de interrupção ampla, o core de destino no site secundário pode recuperar instâncias de máquinas replicadas e iniciar imediatamente a proteção nas máquinas de ativação pós-falha. Depois que o site primário é restaurado, o core replicado pode realizar a reativação pós-falha dos dados a partir das instâncias recuperadas, devolvendo-os às máquinas protegidas no site primário.

Recuperação

A recuperação pode ser realizada no site local ou no site remoto replicado. Quando a implementação está no estado estável com proteção local e replicação opcional, o AppAssure Core permite realizar a recuperação usando Verified Recovery, Universal Recovery ou Live Recovery.

Recursos do produto do AppAssure

Usando o AppAssure, você pode gerenciar todos os aspectos de proteção e recuperação de dados críticos por meio dos seguintes recursos e funcionalidades. Eles incluem:

- Repositório
- True Global Deduplication
- Criptografia
- Replicação
- Recovery-as-a-Service (RaaS)
- Retenção e arquivamento
- Virtualização e nuvem
- Gerenciamento de eventos e alertas
- Portal de licenças
- Console da Web
- APIs de gerenciamento de serviço
- Atribuição de marca branca
- Assistentes AppAssure

Repositório

O repositório do AppAssure usa o gerenciador de volume para deduplicação (DVM) para implementar um gerenciador de volumes que oferece suporte a vários volumes, sendo que cada um deles pode residir em diversas tecnologias de armazenamento, como rede de área de armazenamento (SAN), armazenamento com conexão direta (DAS), armazenamento conectado à rede (NAS) ou armazenamento na nuvem. Cada volume consiste em um armazenamento escalável de objetos com deduplicação. O armazenamento escalável de objetos se comporta como um sistema de arquivos baseado em registros, em que a unidade de alocação de armazenamento é um bloco de dados com tamanho fixo, conhecido como registro. Esta arquitetura permite configurar o suporte do tamanho do bloco para compressão e deduplicação. As operações de rollup são reduzidas a operações de metadados a partir de operações com uso intenso do disco, porque o rollup não movimenta mais os dados, movimenta apenas os registros.

O DVM pode combinar um conjunto de armazenamentos de objetos em um volume, e eles podem ser expandidos pela criação de sistemas de arquivos adicionais. Os arquivos do armazenamento de objetos são pré-alocados e podem ser adicionados sob demanda conforme os requisitos de armazenamento se alteram. É possível criar até 255 repositórios independentes em um único AppAssure Core e aumentar mais o tamanho de um repositório adicionando novas extensões de arquivo. Um repositório estendido pode conter até 4.096 extensões que abrangem diversas tecnologias de armazenamento. O tamanho máximo dos repositórios é 32 Exabytes. Um único core pode ter vários repositórios.

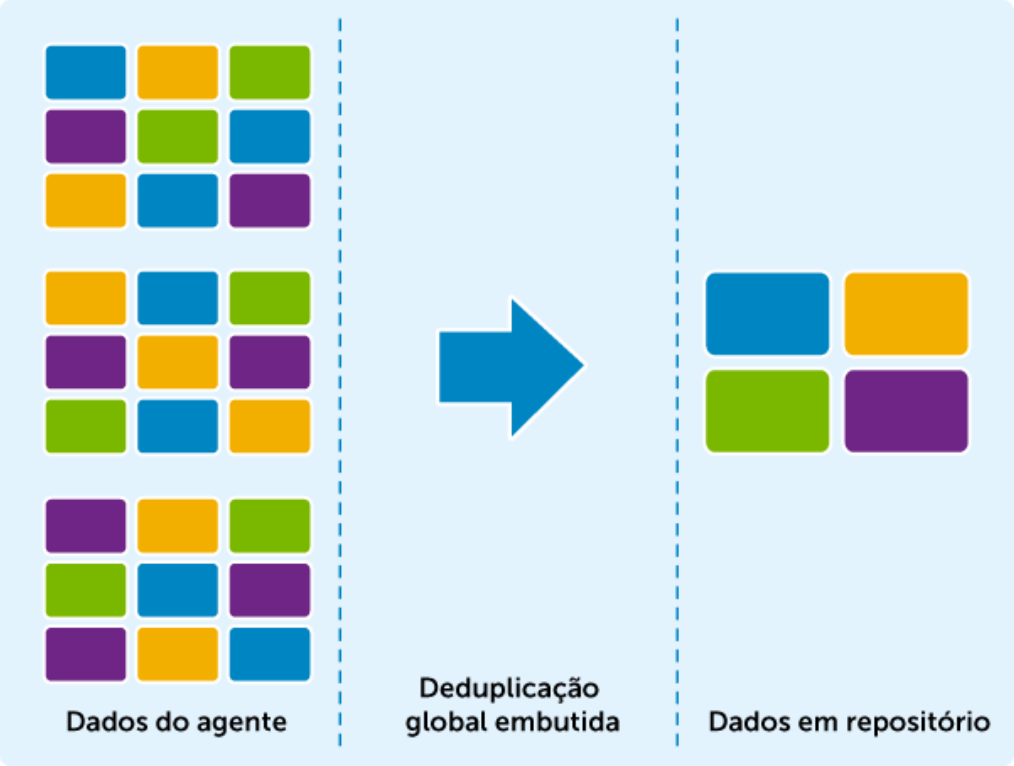
True Global Deduplication

O True Global Deduplication é um método efetivo de redução das necessidades de armazenamento de cópia de segurança, eliminando dados redundantes ou duplicados. A deduplicação é efetiva porque somente uma instância dos dados em várias cópias de segurança é armazenada no repositório. Os dados redundantes são armazenados, mas não fisicamente; eles são simplesmente substituídos por um indicador que aponta para a instância única dos dados no repositório.

Os aplicativos convencionais de cópia de segurança realizam cópias de segurança completas repetitivas semanalmente, mas o AppAssure realiza cópias de segurança incrementais das máquinas no nível do bloco para sempre. Essa abordagem incremental para sempre, em conjunto com a deduplicação de dados, ajuda a reduzir drasticamente o total de dados gravados no disco.

O layout de disco típico de um servidor é constituído pelo sistema operacional, aplicativos e dados. Na maioria dos ambientes, os administradores frequentemente usam um tipo em comum de sistema operacional de desktop e server em vários sistemas, para que a implementação e o gerenciamento sejam efetivos. Quando o AppAssure faz uma cópia de segurança no nível do bloco em várias máquinas ao mesmo tempo, ele fornece uma visualização mais detalhada daquilo que está (e do que não está) na cópia de segurança, independentemente da origem. Esses dados incluem o sistema operacional, os aplicativos e os dados de aplicativo de todo o ambiente.

Figura 4. True Global Deduplication



O AppAssure realiza a deduplicação de dados embutida baseada no destino. Esse método transmite os dados de snapshot para o core antes de serem deduplicados. Deduplicação de dados embutida significa simplesmente que a duplicação dos dados é eliminada antes da confirmação no disco. Isso é muito diferente da deduplicação na origem ou após o processo, na qual a duplicação dos dados é eliminada na origem antes da transmissão; no pós-processo, os dados são enviados em forma bruta para o destino, onde são analisados e a duplicação é eliminada depois da confirmação dos dados no disco. A deduplicação de dados na origem consome recursos preciosos do sistema na máquina, ao passo que a abordagem de eliminação da deduplicação de dados pós-processo requer que todos os dados necessários estejam no disco (uma sobrecarga maior de capacidade inicial) antes de começar o processo de deduplicação. Por outro lado, a deduplicação de dados embutida não requer capacidade de disco adicional e ciclos de CPU na origem nem no Core para o processo de deduplicação. Para concluir, os aplicativos convencionais de cópia de segurança realizam cópias de segurança completas repetitivas toda semana, enquanto que o AppAssure realiza cópias de segurança incrementais das máquinas no nível do bloco para sempre. Essa abordagem incremental para sempre, em conjunto com a deduplicação de dados, ajuda a reduzir drasticamente o total de dados gravados no disco, com uma proporção de redução de até 80:1.

Criptografia

O AppAssure fornece criptografia integrada para proteger cópias de segurança e dados em repouso contra o uso e acesso sem autorização, garantindo a privacidade dos dados. O AppAssure fornece criptografia forte. Ao fazer isso, as cópias de segurança de computadores protegidos ficam inacessíveis. Somente o usuário que tem a chave de criptografia pode acessar e descriptografar os dados. Não há limite para o número de chaves de criptografia que podem ser criadas e armazenadas em um sistema. O DVM usa a criptografia AES de 256 bits no modo encadeamento de blocos de codificação (CBC) com chaves de 256 bits. A criptografia é realizada de forma embutida nos dados de snapshot, a velocidades de linha, sem afetar o desempenho. Isso acontece porque a implementação do DVM é multiprocessamento e usa a aceleração de hardware específica para o processador no qual ele está implementado.

A criptografia está preparada para a multilocação. A deduplicação foi limitada especificamente aos registros que foram criptografados com a mesma chave; dois registros idênticos que foram criptografados com chaves diferentes não terão a deduplicação. Essa decisão de projeto impede que a deduplicação seja usada para vazar dados entre domínios de criptografia diferentes. Isso beneficia os provedores de serviços gerenciados, já que as cópias de segurança replicadas de vários locatários (clientes) podem ser armazenadas em um único core, sem que um locatário possa ver ou acessar os dados de outros locatários. Cada chave de criptografia de um locatário ativo cria um domínio de criptografia dentro do repositório, no qual somente o proprietário das chaves pode ver, acessar ou usar os dados. Em um cenário de multilocação, os dados são particionados e deduplicados dentro dos domínios de criptografia.

Nos cenários de replicação, o AppAssure usa o SSL 3.0 para proteger as conexões entre os dois cores em uma topologia de replicação para impedir espionagem e adulteração.

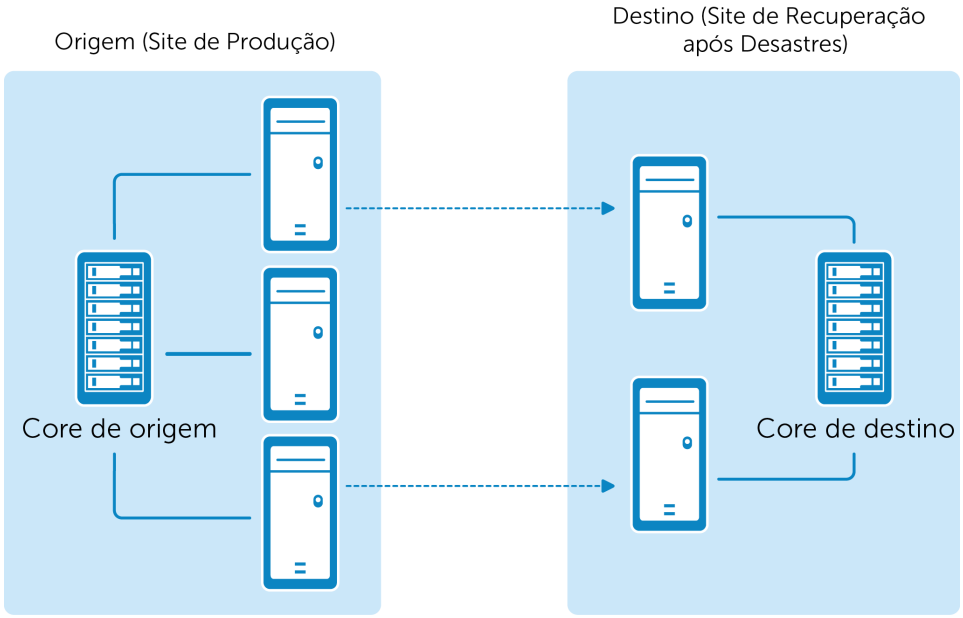
Replicação

Replicação é o processo de copiar pontos de recuperação de um core AppAssure e transmiti-los a outro core AppAssure em um local separado para fins de recuperação após desastres. O processo exige uma solução com pares de origem/destino entre dois ou mais cores.

Esse core de origem copia os pontos de recuperação de máquinas protegidas selecionadas e então transmite de modo assíncrono e contínuo os dados de snapshot incrementais para o core de destino em um site de recuperação após desastres remoto. É possível configurar a replicação de saída para um data center de propriedade da empresa ou para um site de recuperação após desastres remoto (ou seja, um core de destino "autogerenciado"). Ou é possível configurar a replicação de saída para um provedor de serviços gerenciados (MSP) terceirizado ou provedor de nuvem que hospede serviços de recuperação após desastres e cópia de segurança em um site externo. Ao replicar para um core de destino de terceiros, é possível usar fluxos de trabalho incorporados que permitam solicitar conexões e receber notificações automáticas de feedback.

A replicação é gerenciada por máquina protegida. Qualquer máquina (ou todas as máquinas) protegida ou replicada em um core de origem pode ser configurada para replicar em um core de destino.

Figura 5. Replicação



A replicação se otimiza com um algoritmo exclusivo de leitura-correspondência-gravação (RMW) acoplado fortemente à deduplicação. Na replicação RMW, o serviço de replicação de origem e destino faz a correspondência das chaves antes de transferir dados e, em seguida, replica somente os dados compactados, criptografados e de deduplicação pela WAN. Ao fazer isso, reduz em 10x os requisitos de largura de banda.

A replicação começa pela propagação, ou seja, a transferência inicial de imagens de base de deduplicação e snapshots incrementais dos agentes protegidos, que pode acrescentar centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada para o core de destino usando mídias externas. Normalmente, isso é útil para grandes conjuntos de dados ou sites com links lentos. Os dados do arquivo de propagação são compactados e criptografados e a duplicação é eliminada. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo pode ocupar vários dispositivos, com base no espaço disponível nas mídias. Durante o processo de propagação, os pontos de recuperação incremental são replicados no site de destino. Depois que o core de destino consome o arquivo de propagação, os pontos de recuperação incremental recém-replicados são sincronizados automaticamente.

Recovery-as-a-Service (RaaS)

Os provedores de serviços gerenciados (MSPs) podem utilizar o AppAssure como uma plataforma para oferecer a recuperação como serviço (RaaS). A RaaS facilita a recuperação completa na nuvem replicando os servidores físicos e virtuais do cliente, juntamente com seus dados, para a nuvem do provedor de serviços como máquinas virtuais para suportar o teste de recuperação ou operações reais de recuperação. Os clientes que desejam realizar recuperação na nuvem podem configurar a replicação nas máquinas protegidas nos cores locais para um provedor de serviços do AppAssure. Em caso de desastre, os MSPs podem realizar instantaneamente o provisionamento das máquinas virtuais para o cliente.

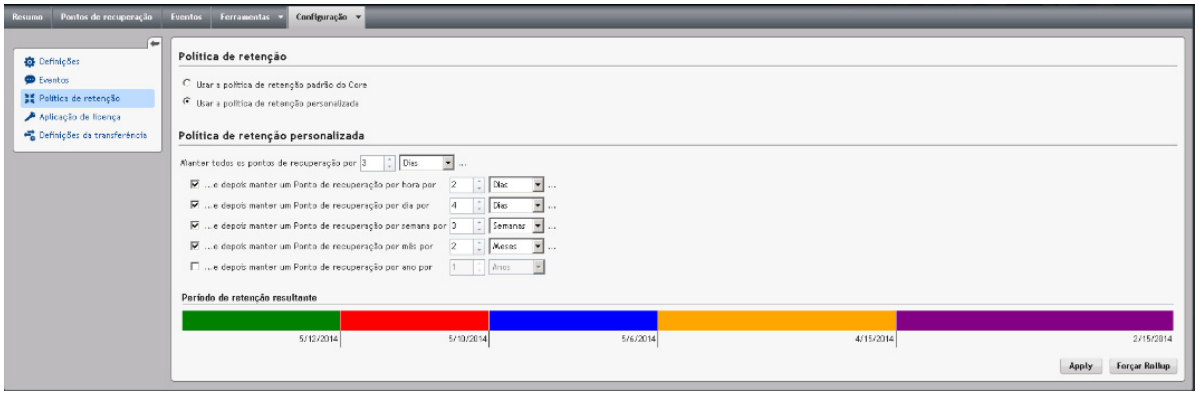
Os MSPs podem implementar uma infraestrutura de RaaS com multilocação baseada em AppAssure que pode hospedar várias organizações ou unidades de negócios separadas (os locatários), que normalmente não compartilham segurança ou dados em um único servidor ou um grupo de servidores. Os dados de cada locatário são isolados e protegidos de outros locatários e do provedor de serviço.

Retenção e arquivamento

O AppAssure oferece políticas flexíveis de cópia de segurança e retenção fáceis de configurar. A capacidade de ajustar as políticas de retenção às necessidades de uma organização não só ajuda a preencher os requisitos de conformidade, mas também faz isso sem comprometer os objetivos de tempo de recuperação (RTO).

As políticas de retenção impõem períodos de tempo em que as cópias de segurança são armazenadas em mídias de curto prazo (rápidas e caras). Às vezes, certos requisitos técnicos e de negócios exigem a retenção prolongada dessas cópias de segurança, mas o armazenamento rápido tem um custo proibitivo. Portanto, esse requisito gera uma necessidade de armazenamento de longo prazo (lento e barato). As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados de conformidade e não conformidade. O recurso de arquivamento suporta retenções prolongadas para dados de conformidade e não conformidade, além de ser usado para propagar dados de replicação para um core de destino.

Figura 6. Política de retenção


Resumo
Pontos de recuperação
Eventos
Ferramentas
Configuração
Definições
Eventos
Política de retenção
Aplicação de licença
Definições da transferência
Política de retenção
Usar a política de retenção padrão do Core
Usar a política de retenção personalizada
Política de retenção personalizada
Manter todos os pontos de recuperação por 3 Dias
...e depois manter um Ponto de recuperação por hora por 2 Dias
...e depois manter um Ponto de recuperação por dia por 4 Dias
...e depois manter um Ponto de recuperação por semana por 3 Semanas
...e depois manter um Ponto de recuperação por mês por 2 Meses
...e depois manter um Ponto de recuperação por ano por 1 Anos
Período de retenção resultante
5/12/2014
5/10/2014
5/6/2014
4/15/2014
2/15/2014
Apply
Forçar Rollup

No AppAssure, as políticas de retenção podem ser personalizadas para especificar o tempo durante o qual um ponto de recuperação de cópia de segurança é mantido. Conforme o fim do período de retenção dos pontos de recuperação se aproxima, eles vencem e são removidos do grupo de retenção. Normalmente, esse processo se torna ineficiente e acaba falhando, já que a quantidade de dados e o período de retenção começam a aumentar rapidamente. O AppAssure resolve o problema do big data gerenciando a retenção de grandes quantidades de dados com políticas de retenção complexas e realizando operações de rollup para dados que estão vencendo, por meio de operações eficientes de metadados.

É possível realizar cópias de segurança com um intervalo de poucos minutos, e essas cópias de segurança vencem em dias, meses e anos. As políticas de retenção gerenciam o vencimento e a exclusão de cópias de segurança antigas. Um método simples em cascata define o processo de vencimento. Os níveis dentro da cascata são definidos em minutos, horas e dias; semanas, meses e anos. A política de retenção é imposta pelo processo noturno de rollup.

Para o arquivamento de longo prazo, o AppAssure permite criar um arquivo do core de origem ou destino em qualquer mídia removível. O arquivo é otimizado internamente, e todos os dados do arquivo são compactados, criptografados e têm deduplicação. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo ocupará vários dispositivos com base no espaço disponível nas mídias. A recuperação a partir de um arquivo não requer um novo core; qualquer core pode ingerir o arquivo e recuperar dados se o administrador tiver a frase de acesso e as chaves de criptografia.

Virtualização e nuvem

O AppAssure Core está preparado para a nuvem, permitindo que você utilize a capacidade computacional da nuvem para a recuperação e para o arquivamento.

O AppAssure pode exportar qualquer máquina protegida ou replicada para uma máquina virtual (VM), como a versão licenciada do VMware ou Hyper-V. É possível realizar uma exportação virtual de uma vez ou estabelecer uma máquina virtual em modo de standby virtual ao estabelecer uma exportação virtual contínua. Nas

exportações contínuas, a máquina virtual é atualizada de forma incremental depois de cada snapshot. As atualizações adicionais são rápidas e fornecem clones em estado de espera prontos para serem acionados com um clique em um botão. Tipos de exportação de VM suportados incluem: VMware Workstation e VMWare Server em uma pasta; exportação direta para um host do vSphere ou VMware ESX(i); exportação para o Oracle VirtualBox; e exportação para o Microsoft Hyper-V Server no Windows Server 2008 (x64), 2008 R2, 2012 (x64) e 2012 R2 (incluindo suporte para as máquinas virtuais Hyper-V geração 2).

Além disso, é possível arquivar seus dados do repositório na nuvem utilizando o Microsoft Azure, Amazon S3, Rackspace Cloud Files ou outros serviços de nuvem baseados em OpenStack.

Gerenciamento de eventos e alertas

Além das APIs de REST HTTP, o AppAssure também inclui um conjunto amplo de recursos para a criação de logs e a notificação de eventos usando e-mail, syslog ou o Log de eventos do Windows. As notificações por e-mail podem ser usadas para alertar os usuários ou grupos sobre o funcionamento ou o status de diversos eventos em resposta a um alerta. Os métodos do syslog e do Log de Eventos do Windows são usados para a criação de logs centralizada em um repositório, em ambientes com vários sistemas operacionais; por outro lado, em ambientes que só têm Windows, apenas o Log de Eventos do Windows é usado.

Portal de licenças

O Portal de licenças do Dell AppAssure fornece ferramentas fáceis de usar para gerenciar os direitos de licença. É possível baixar, ativar, ver e gerenciar chaves de licença e criar um perfil de empresa para rastrear os ativos de licença. Além disso, o portal permite que os provedores de serviços e revendedores rastreiem e gerenciem as licenças de cliente.

Console da Web

O AppAssure tem um console central baseado na Web que gerencia cores distribuídos do AppAssure a partir de um local central. Os provedores de serviços gerenciados (MSPs) e clientes corporativos com vários cores distribuídos podem implementar esse console para obter uma visualização unificada para um gerenciamento centralizado. O AppAssure Central Management Console permite organizar os cores gerenciados em unidades organizacionais hierárquicas. Essas unidades organizacionais podem representar unidades de negócios, locais ou clientes para os MSPs com acesso baseado em função. Usando o console central, você também pode executar relatórios em todos os cores gerenciados.

APIs de gerenciamento de serviço

O AppAssure vem com um conjunto de APIs de gerenciamento de serviços e fornece acesso programático a todas as funcionalidades disponíveis por meio do AppAssure Central Management Console. A API de gerenciamento de serviços é uma API de REST. Todas as operações de API são realizadas em SSL e autenticadas mutuamente por meio de certificados X.509 v3. O serviço de gerenciamento pode ser acessado de dentro do ambiente ou diretamente pela Internet, a partir de qualquer aplicativo que possa enviar e receber solicitações e respostas de HTTPS. A abordagem facilita a integração fácil a qualquer aplicativo da Web, como ferramentas de metodologia de gerenciamento de relacionamentos (RMM) ou sistemas de faturação. Um cliente de SDK para PowerShell scripting também está incluído no AppAssure.

Atribuição de marca branca

O AppAssure pode ter a marca alterada ou ser comercializado sem marca para parceiros corporativos e de OEM selecionados, de acordo com o programa de provedor de serviços Platinum. Com o programa de provedor de serviços Platinum, os parceiros podem usar seu nome, logotipo e cores no AppAssure e fornecer o produto ou serviço com sua própria marca e visual para os clientes.

Como parceiro do AppAssure, você pode ajustar o software para que ele atenda aos seus requisitos de negócios. Para saber mais sobre a forma de uso da sua marca no AppAssure visando a suprir as suas necessidades de negócios, entre em contato com o Departamento de Vendas Dell AppAssure pelo e-mail sales@software.dell.com para obter mais informações.

Assistentes AppAssure

O assistente é um conjunto de etapas guiadas apresentadas ao usuário em uma janela pop-up para automatizar uma tarefa complexa ou mais. Por definição, os assistentes contêm duas páginas de informações (ou mais) para o usuário preencher. (Um pop-up de janela única é considerado simplesmente como uma caixa de diálogo). Os assistentes usam diversas convenções gráficas bastante conhecidas para coletar informações, como caixas de texto, botões de opções, caixas de verificação e menus suspensos.

Quando um assistente é iniciado, uma janela se abre acima da interface do usuário e o orienta em uma série de opções necessárias para realizar a tarefa. Você segue as informações apresentadas em cada página do assistente, conforme os seus requisitos, navegando pelas páginas do assistente por meio dos botões **Avançar** e **Voltar**. Ao terminar, você clica em um botão de enviar (para confirmar suas opções e realizar a tarefa) ou no botão **Cancelar** (para cancelar sem fazer alterações e voltar à UI na qual você abriu o assistente).

O AppAssure oferece vários assistentes, que podem ser divididos em duas categorias.

Primeiramente, há assistentes para instalar, atualizar ou remover o software AppAssure e os componentes relacionados. Normalmente, eles são iniciados ao clicar duas vezes em um programa executável de instalador de software. Os instaladores podem ser acessados ao fazer o download de componentes específicos do Portal de licenças do Dell AppAssure.

Em segundo lugar, os assistentes estão disponíveis na interface de usuário do AppAssure Core Console. Normalmente, eles são lançados ao clicar em um botão ou link rotulado com a função ou o resultado do assistente. Os assistentes dessa categoria são listados a seguir.

Tabela 1.

Nome do assistente	Iniciado por	Descrição
Guia de início rápido	Opção Guia de início rápido (menu Ajuda)	Unifica vários fluxos de trabalho para simplificar tarefas comuns do AppAssure. Guia o usuário no processo de proteger máquinas, configurar a replicação em novos agentes, exportar dados protegidos para máquinas virtuais, criptografar dados dos pontos de recuperação, configurar grupos de notificação por e-mail e configurar uma política de retenção.
Assistente de proteção de máquina	Botão Proteger máquina (barra de botões)	Configura a proteção em uma máquina que você especifica. Permite dar um nome à máquina para ser exibido no console do Core. Se o software Agent já estiver instalado, ele permite selecionar volumes para a proteção. Caso contrário, o assistente instalará o software e protegerá todos os volumes. Configura uma programação padrão de proteção ou permite configurar uma programação personalizada. Nas definições avançadas, é possível escolher (ou criar) um repositório e estabelecer a criptografia para os dados protegidos.
Assistente de proteção de diversas máquinas	Botão Proteção em massa (guia Inicial)	Configura a proteção em várias máquinas que você especifica, a partir de um servidor de domínio do Active Directory do Windows, um host virtual do VMware vCenter Server/ESX(i) ou manualmente (inserindo uma lista em um formato especificado).

Tabela 1.

Nome do assistente	Iniciado por	Descrição
Assistente de replicação	Link Adicionar core de destino (guia Replicação)	Configura a replicação a partir de um core primário (ou de origem) para que uma cópia dos dados protegidos esteja sempre disponível em um core de destino separado.
Assistente de restauração de máquina	Botão Restaurar (barra de botões)	Orienta você durante o processo de restaurar dados a partir de um ponto de recuperação no Core para uma máquina protegida, ou ao iniciar uma bare metal restore.
Assistente de exportação	Botão Exportar (barra de botões), link Adicionar (guia Standby virtual)	Exporta dados do ponto de recuperação de uma máquina protegida para uma máquina virtual em qualquer formato de VM suportado. É possível realizar uma exportação única ou configurar o standby virtual para a exportação contínua.

Normalmente, os assistentes instalam ou configuram recursos no AppAssure, mas é possível modificar posteriormente a maioria desses aspectos no Core Console.

2

Instalação e configuração do AppAssure Add-on for Kaseya e do software do AppAssure

Este capítulo descreve como instalar e configurar AppAssure Add-on for Kaseya Management Console, bem como o software do AppAssure Core e do AppAssure Agent. Os seguintes tópicos estão incluídos:

- Preparar o AppAssure Add-on for Kaseya
- Instalação do AppAssure Add-on for Kaseya
- Desinstalação do AppAssure Add-on for Kaseya
- Requisitos do sistema do AppAssure
- Gerenciamento de suas licenças do AppAssure
- Instalação do AppAssure usando o Kaseya

O AppAssure Add-on for Kaseya é um plug-in de software que se integra com a interface de gerenciamento do sistema Kaseya para instalar e monitorar agentes de cópia de segurança em toda a sua base de clientes. Com o AppAssure Add-on for Kaseya, é possível fazer o seguinte:

- Implementar o AppAssure Agent e o Core
- Proteger máquinas
- Configurar uma replicação
- Realizar relatórios consolidados

Os recursos de recuperação não estão disponíveis no Kaseya Management Console, mesmo com o AppAssure Add-on instalado. Para visualizar e explorar os pontos de recuperação, ou para realizar uma restauração, é preciso fazer isso a partir da máquina em que o AppAssure Core está instalado, usando o AppAssure Core Console. Para obter mais informações sobre o uso do AppAssure Core Console, consulte o *Guia do usuário do Dell AppAssure*.

Preparar o AppAssure Add-on for Kaseya

Há um processo de várias etapas para garantir que o AppAssure Add-on integre-se ao Kaseya. Ele envolve instalar o software do Add-on no seu servidor Kaseya e então implementar o AppAssure Core e o AppAssure Agent nas máquinas que deseja incluir. Em seguida, você deve definir as credenciais e os repositórios para as máquinas ou os servidores que deseja proteger.

Para configurar o AppAssure for Kaseya, realize as seguintes etapas:

- Etapa 1: Instale o AppAssure Add-on for Kaseya no seu servidor Kaseya. Para obter mais informações, consulte Instalação do AppAssure Add-on for Kaseya.
- Etapa 2: Acesse o Portal de licenças do AppAssure em https://licenseportal.com e crie uma conta. Para obter mais informações, consulte o *Guia do usuário do Portal de licenças do Dell AppAssure*.
- Etapa 3: Use a chave de licença obtida do Portal de licenças do AppAssure para criar uma licença. Para obter mais informações, consulte Criação de uma licença do AppAssure.

- Etapa 4: Implemente e instale o software AppAssure Core e Agent. Para obter mais informações, consulte Instalação do AppAssure usando o Kaseya.
- Etapa 5: Configure as credenciais para o Core e as máquinas protegidas. Para obter mais informações, consulte Gerenciamento de credenciais do AppAssure Core e do agente.
- Etapa 6: Crie e atribua um repositório para armazenar os dados da cópia de segurança. Para obter mais informações, consulte Configuração de repositórios.
- Etapa 7: Comece a proteger suas máquinas. Para obter mais informações, consulte Configuração da proteção de máquina.

Instalação do AppAssure Add-on for Kaseya

A instalação do AppAssure Add-on envolve instalar o software AppAssure Add-on no seu servidor Kaseya conforme descrito nesta seção e depois instalar e implementar os serviços AppAssure Core e Agent em máquinas com Windows, conforme descrito na seção Instalação do AppAssure usando o Kaseya.

NOTA: Para instalar o AppAssure Add-on for Kaseya, navegue para o URL recebido da Dell para baixar o arquivo do instalador do Add-on para o seu sistema. O AppAssure Add-on exige a versão 6.2 ou mais recente do servidor Kaseya.

Para instalar o AppAssure Add-on for Kaseya

1. Em seu sistema, acesse e clique duas vezes no arquivo do instalador do AppAssure Add-on for Kaseya. O Assistente do InstallShield será iniciado.
   - Se for exibida uma janela indicando Abrir arquivo - Aviso de segurança, clique em **Executar** para continuar.
2. Na página Bem-Vindo, clique em **Avançar** para prosseguir com a instalação.
3. Na página Acordo de licença, selecione **Eu aceito os termos do acordo de licença** e, em seguida, clique em **Avançar**.
4. Na página Pronto para instalar o programa, clique em **Instalar**.

   NOTA: No caso raro de sua instância do Microsoft Internet Information Services (IIS) atender a outros websites, esses sites ficarão temporariamente indisponíveis até que a instalação do AppAssure seja concluída.

   Uma página será exibida com o status e o progresso da instalação.
5. Como opção, na página Assistente de instalação concluída, selecione Mostrar o log do Windows Installer.
6. Clique em **Concluir**.

   Agora você pode efetuar login no Kaseya para selecionar o AppAssure Add-on e implementar o software AppAssure em seus servidores compatíveis. Para obter uma lista de sistemas suportados, consulte Requisitos do sistema do AppAssure.

Desinstalação do AppAssure Add-on for Kaseya

Se for necessário desinstalar o Kaseya Add-on do AppAssure, é preciso fazer isso no servidor Kaseya designado.

Para desinstalar o Kaseya Add-on

1. No servidor Kaseya, localize a pasta AA5AddonForKaseya (por exemplo, C:\Users\Administrator\Downloads\AA5AddonForKaseya ou usando a opção Programas e Recursos no Painel de Controle do Windows).

- Se for exibida uma janela indicando Abrir arquivo - Aviso de segurança, clique em **Executar** para continuar.

2 Na pasta AA5AddonForKaseya, clique duas vezes no arquivo do aplicativo AppAssure AddonForKaseya-5.4.x.xxx.

3 Na primeira página do Installation Wizard, clique em **Avançar**.

4 Na página de Gerenciamento do programa, selecione **Remover** e clique em **Avançar**.

5 Na página Remover o programa, clique em **Remover**.

O Installation Wizard remove o programa do servidor Kaseya.

6 Depois de o assistente concluir a remoção, clique em **Concluir**.

Requisitos do sistema do AppAssure

Instale o AppAssure Core em um servidor Windows de 64 bits dedicado. Para cada máquina que desejar proteger com o AppAssure Core, instale a versão do software do AppAssure Agent adequada ao sistema operacional da máquina. Dependendo de sua licença e dos requisitos do seu ambiente, pode ser preciso instalar diversos cores. E, opcionalmente, para o gerenciamento remoto de diversos cores, você pode instalar o AppAssure Central Management Console em um computador Windows de 64 bits.

Antes de instalar o AppAssure, verifique se seu sistema atende aos seguintes requisitos mínimos de hardware e software.

△ **CUIDADO: A Dell não suporta a execução do AppAssure Core em sistemas operacionais Windows Core, os quais oferecem funções de servidor limitadas. Essa limitação inclui todas as edições do Windows Server 2008 Core, Windows Server 2008 R2 Core, Windows Server 2012 Core e Windows Server 2012 R2 Core. Os seguintes sistemas operacionais são suportados para a execução do software AppAssure Agent.**

CUIDADO: A Dell não recomenda a execução do AppAssure 5 Core na mesma máquina física que atua como o host do Hyper-V. (Essa recomendação não se aplica a appliances de cópia de segurança e recuperação da Dell).

Tabela 2. Requisitos do sistema

Componente do AppAssure	Requisito	Detalhes
AppAssure Core e AppAssure Central Management Console	Sistema operacional	• Microsoft Windows 7 (todas as edições x64) • Microsoft Windows 8* (todas as edições x64) • Microsoft Windows 8.1* (todas as edições x64) • Microsoft Windows Server 2008 (todas as edições x64 **exceto** Windows Server 2008 Core) • Microsoft Windows Server 2008 (todas as edições x64 **exceto** Windows Server 2008 R2 Core) • Microsoft Windows Server 2012* (todas as edições x64 **exceto** Windows Server 2012 Core) • Microsoft Windows Server 2012 R2* (todas as edições x64 **exceto** Windows Server 2012 R2 Core) **NOTA:** Os sistemas operacionais Windows requerem que o .NET Framework 4.0x esteja instalado para executar o serviço AppAssure Core. Além disso, os sistemas operacionais marcados com * exigem a função/recurso ASP .NET 4.5x. Ao instalar ou atualizar o AppAssure Core, o instalador irá verificar esses componentes com base no OS do servidor Core e irá instalá-los automaticamente, se necessário. Para obter um desempenho ideal, recomenda-se instalar o AppAssure Core no Windows 8.1 (ou mais recente) e Windows Server 2012 (ou mais recente). O AppAssure Core exige o uso de uma plataforma de 64 bits do Windows. Sistemas de 32 bits e sistemas Linux não são suportados.
	Arquitetura	Somente 64 bits
	Memória	8 GB RAM ou superior. A Dell recomenda fortemente o uso da memória ECC (Verificação e correção de erros) para garantir o desempenho ideal dos servidores do AppAssure Core.
	Processador	Quad-core ou superior.
	Armaze-namento	Armazenamento por conexão direta, Rede de área de armazenamento ou Armazenamento conectado à rede.
	Rede	1 GB ou superior

Tabela 2. Requisitos do sistema

Componente do AppAssure	Requisito	Detalhes
AppAssure Agent	Sistema operacional	• Microsoft Windows XP SP3 (Professional Edition apenas) • Microsoft Windows Vista (todas as edições) • Microsoft Windows 7 (todas as edições) • Microsoft Windows 8* (todas as edições) • Microsoft Windows 8.1* (todas as edições) • Microsoft Windows Server 2003 (todas as edições) • Microsoft Windows Server 2008 (todas as edições) • Microsoft Windows Server 2008 R2 (todas as edições) • Microsoft Windows Server 2008 R2 SP1 Core (todas as edições) • Microsoft Windows Server 2012* (todas as edições) • Microsoft Windows Server 2012 R2* (todas as edições) • Microsoft Windows Storage Server 2012* (todas as edições) • Microsoft Windows Storage Server 2012 R2* (todas as edições) • Red Hat Enterprise Linux (RHEL) 6.3 • RHEL 6.4 • RHEL 6.5 • RHEL 7 x64 • CentOS Linux 6.3 • CentOS Linux 6.4 • CentOS Linux 6.5 • CentOS Linux 7 x64 • Ubuntu Linux 12.04 LTS • Ubuntu Linux 13.04 • Ubuntu Linux 14.04 • SUSE Linux Enterprise Server (SLES) 11 SP2 • SLES 11 SP3 **NOTA:** Os sistemas operacionais Windows requerem que o Microsoft .NET Framework (4.0x) esteja instalado para executar o serviço AppAssure Agent. **NOTA:** Oferecemos suporte às distribuições do Linux na lista acima e realizamos testes com a maioria das versões lançadas do kernel. **NOTA:** Agents instalados no Microsoft Hyper-V Server 2012 funcionam no modo de edição do Core do Windows Server 2012. **NOTA:** Em agentes Linux, o AppAssure suporta somente os seguintes sistemas de arquivo: ext3, ext4 e xfs. **NOTA:** A cópia de segurança nativa do Cluster Shared Volumes é suportada somente nos agentes do Windows 2008 R2.
	Arquitetura	32 bits ou 64 bits
	Memória	4 GB ou superior
	Suporte do Microsoft Exchange	• Microsoft Exchange 2007 SP1 Rollup 5 ou mais recente • Microsoft Exchange 2010 • Microsoft Exchange 2013
	Suporte Microsoft SQL	• Microsoft SQL Server 2005 • Microsoft SQL Server 2008 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014

Para obter mais informações sobre o uso do AppAssure, consulte o Guia do usuário do *Dell AppAssure*. Para obter mais informações sobre o gerenciamento de licenças do Dell AppAssure, consulte o Guia do usuário do *Portal de licenças do Dell AppAssure*. Para obter mais informações sobre dimensionamento de seu hardware, software, memória, armazenamento e requisitos de rede, consulte o artigo da Knowledgebase Dell AppAssure 118407, "Dimensionando implantações do AppAssure".

Gerenciamento de suas licenças do AppAssure

Antes de baixar os pacotes de instalação do AppAssure Core e Agent, efetue login no Portal de licenças do Dell AppAssure em https://licenseportal.com e registre-se para uma conta. Então é possível baixar o instalador e obter uma chave de licença para ativar o software. Para obter mais informações sobre o Portal de licenças do Dell AppAssure, consulte o *Guia do usuário do portal de licenças do Dell AppAssure*, localizado no site de documentação de Guias e notas de versão do AppAssure em https://support.software.dell.com/appassure/release-notes-guides.

Após a instalação do AppAssure Core, você pode baixar o AppAssure Agent Installer a partir do Core ou do Portal de licenças do Dell AppAssure para cada máquina que o Core protege.

Criação de uma licença do AppAssure

Execute o procedimento a seguir para inserir a chave de licença necessária para implementar o software AppAssure dentro do Kaseya.

Para criar uma licença do AppAssure

1 Navegue até a seção Implementação do AppAssure e selecione **Gerenciar licenças**.

2 Insira as seguintes informações de sua licença.

Tabela 3.

Caixa de texto	Descrição
Nome da licença	Um nome descritivo para identificar a licença.
Chave de licença	A chave de licença que você recebeu da equipe de licenciamento do Dell Software Group.
Descrição	(opcional) Uma descrição para a chave de licença.

3 Clique em **Criar licença**.

4 Repita as etapas anteriores para todas as licenças que você deseja inserir.

Todas as licenças adicionadas serão exibidas na tabela Licença desta página.

Exclusão de licenças do AppAssure

Execute o procedimento a seguir para excluir licenças do AppAssure.

Para excluir licenças do AppAssure

1 Navegue até a seção Implementação do AppAssure e selecione **Gerenciar licenças**.

2 Na tabela Licenças, selecione as licenças que você deseja excluir.

3 Clique em **Excluir licenças**.

Instalação do AppAssure usando o Kaseya

O AppAssure Core armazena e gerencia as cópias de segurança de todos os servidores ou máquinas protegidos no seu ambiente - em que o AppAssure Agent está instalado.

Para começar, é preciso baixar o pacote do instalador do AppAssure Core Web (que inclui o software AppAssure Agent) no Portal de licenças do Dell AppAssure em https://licenseportal.com. Salve o arquivo em um local de fácil acesso em seu sistema para que futuramente você possa enviá-lo ao Kaseya Server.

Após a conclusão da instalação do AppAssure Core, você poderá acessar o arquivo do AppAssure Agent Installer no seu sistema em:

```
C:\Program Files\AppRecovery\Core\Installers
```

NOTA: Somente versões 5.3.1.x ou mais recentes do software AppAssure Core ou Agent são suportadas.

Depois de baixar o instalador, execute as seguintes etapas:

- Etapa 1: Carregamento de um pacote de instalação do AppAssure no servidor Kaseya
- Etapa 2: Implementação do AppAssure Core
- Etapa 3: Instalação do software do AppAssure Agent
- Etapa 4: Verificação da instalação do AppAssure em uma máquina

Carregamento de um pacote de instalação do AppAssure no servidor Kaseya

Depois de instalar o AppAssure Add-on, é possível usá-lo para implementar o AppAssure Core e Agent nas máquinas que deseja proteger.

NOTA: Somente versões 5.3.1.x ou mais recentes do software AppAssure Core ou Agent são suportadas.

Para carregar um pacote de instalação do AppAssure no servidor Kaseya

1. Navegue até a seção Implementação do AppAssure no Kaseya e clique em **Carregar pacotes**.
2. Clique no botão **Procurar um arquivo** para localizar o arquivo do pacote de instalação da Web do AppAssure Core Web ou AppAssure Agent em seu sistema.
3. Na caixa de diálogo, selecione o arquivo de instalação do Core no seu sistema e clique em **Abrir**.
4. Clique em **Carregar arquivo**.

Implementação do AppAssure Core

É possível usar a interface do AppAssure Add-on for Kaseya para implementar e instalar o AppAssure Core em servidores em rede. Execute o procedimento a seguir para implementar o AppAssure Core.

CUIDADO: Ao realizar o upgrade de uma máquina para uma versão mais recente do AppAssure, sempre realize o upgrade do Core antes do Agent. Se tiver replicação ativada, é importante implementar o upgrade do AppAssure na seguinte ordem: core de destino, core de origem e agente.

Para implementar o AppAssure Core

1. Navegue até a seção Implementação do AppAssure e clique em **Instalar Cores** para instalar o AppAssure em suas máquinas.

2 Especifique as seguintes opções para definir quando e como instalar o software.

Tabela 4.

Opção	Descrição
Executar agora	Selecione esta opção para executar a instalação agora.
Programado	Selecione esta opção para programar um horário para a execução da instalação. Selecione as seguintes opções nas quatro listas suspensas para programar um horário para executar a instalação: • A combinação de mês e ano • O dia • A hora • O minuto da hora
Ajustar em	(opcional) Use essa opção se for atualizar o software do Core em várias máquinas. Insira um número em minutos para ajustar o horário em que cada máquina tenta executar a atualização para uniformizar a carga nos servidores de arquivos e na conexão com a Internet.
Ignorar caso a máquina esteja offline	(opcional) Selecione esta opção para examinar apenas no horário agendado. Se a máquina estiver offline, ignore esta opção e reagende a instalação para o próximo intervalo. Desmarque esta caixa de seleção para examinar logo que a máquina se conectar após o horário agendado.

3 Na lista suspensa **Escolher pacote de instalação do AppAssure 5**, selecione a versão do Core que deseja instalar.

4 No menu suspenso Escolher uma licença, selecione a licença adicionada para o Core que está sendo implementado.

5 Na lista de máquinas nesta página, selecione as máquinas nas quais você deseja implementar o software AppAssure Core.

6 Clique em **Instalar/Reinstalar**.

7 Na janela Confirmar, clique em **Sim**.

Quando a instalação começar, uma mensagem será exibida na coluna Versão do AppAssure Core 5 das máquinas afetadas, avisando sobre o início da instalação. Quando a instalação for concluída, a versão do software do Core instalada será exibido nesta coluna.

NOTA: Selecione uma máquina na lista para iniciar o recurso Kaseya, Live Connect, para essa máquina.

Instalação do software do AppAssure Agent

Esta seção descreve as etapas necessárias para instalar e implementar o software AppAssure Agent nas máquinas do seu ambiente.

NOTA: Se o AppAssure Core ou Agent já estiver instalado na máquina de destino, uma atualização ou um reparo será realizado. Observe que não é possível fazer o downgrade de uma instalação para uma versão anterior.

CUIDADO: Ao realizar o upgrade de uma máquina para uma versão mais recente do AppAssure, sempre realize o upgrade do Core antes do Agent. Se tiver replicação ativada, é importante implementar o upgrade do AppAssure na seguinte ordem: core de destino, core de origem e agente.

Para instalar o software AppAssure Agent

1 Navegue até a seção Implementar o AppAssure e clique em **Instalar Agents** para instalar o AppAssure em suas máquinas.

2 Especifique as seguintes opções para definir quando e como instalar o software.

Tabela 5.

Opção	Descrição
Executar agora	Selecione esta opção para executar a instalação agora.
Programado	Selecione as seguintes opções nas quatro listas suspensas para programar um horário para executar a instalação: • A combinação de mês e ano • O dia • A hora • O minuto da hora
Ajustar em	(opcional) Use essa opção quando atualizar o software. Insira um número em minutos para ajustar o horário em que cada máquina tenta executar a atualização para uniformizar a carga nos servidores de arquivos e na conexão com a Internet.
Ignorar caso a máquina esteja offline	(opcional) Selecione esta opção para examinar apenas no horário agendado. Se a máquina estiver offline, ignore esta opção e reagende a instalação para o próximo intervalo. Desmarque esta caixa de seleção para examinar logo que a máquina se conectar após o horário agendado.

3 Na lista suspensa **Escolher pacote de instalação do AppAssure 5**, selecione a versão do software do AppAssure Agent que deseja instalar.

4 Na lista de máquinas nesta página, selecione as máquinas nas quais você deseja implementar o software AppAssure Agent.

> **DICA:** Ao realizar o upgrade, na página Preparar replicação na árvore de navegação, verifique o Core que protege cada agente e se você não está realizando o upgrade de um agente antes de um core.

5 Clique em **Instalar/Reinstalar**.

6 Na janela Confirmar, clique em **Sim**.

Quando a instalação começar, uma mensagem será exibida na coluna Versão do AppAssure Agent 5 das máquinas afetadas, avisando que o processo de instalação foi iniciado. Quando a instalação for concluída, o número da versão do software AppAssure Agent instalado será exibido nesta coluna.

> **NOTA:** Selecione uma máquina na lista para iniciar o recurso Kaseya, Live Connect, para essa máquina.

Verificação da instalação do AppAssure em uma máquina

Execute o procedimento a seguir para confirmar a instalação do AppAssure em uma máquina específica.

Para confirmar a instalação do AppAssure em uma máquina

1 Na lista de máquinas da página Instalar Agents ou Instalar Cores, selecione a máquina e clique em **Confirmar instalação**.

2 Na janela Confirmar, clique em **Sim**.

Uma mensagem é exibida ao lado da máquina alertando que uma auditoria está sendo realizada. Essa auditoria verifica se um core ou agente está instalado na máquina selecionada e lista a versão do software na coluna Versão do AppAssure.

Se nenhuma versão estiver instalada, um texto indicando que a instalação não ocorreu é exibido na coluna de versão do AppAssure (Versão do AppAssure Core 5 para cores, Versão AppAssure 5 Agent para agentes).

3

Uso do AppAssure Add-on for Kaseya

Este capítulo descreve como usar o AppAssure Add-on for Kaseya para proteger e replicar máquinas. Os seguintes tópicos estão incluídos:

- Gerenciamento de credenciais do AppAssure Core e do agente
- Configuração de repositórios
- Configuração da proteção de máquina
- Gerenciamento da replicação
- Monitoramento da atividade do AppAssure
- Gerenciamento de relatórios do AppAssure Core

O AppAssure Add-on for Kaseya permite realizar várias funções do AppAssure diretamente no Kaseya Management Console. Use a árvore de navegação na coluna Cópia de Segurança do Servidor AppAssure 5 do console para acessar as várias páginas do AppAssure.

A árvore de navegação do AppAssure inclui os seguintes nós-raiz:

- **Bem-vindo ao AppAssure 5.** Uma visão geral do produto.
- **Implementação do AppAssure.** Carregue versões de software, gerencie licenças e implemente o software AppAssure.
- **Configurar gerenciamento.** Visualize e gerencie credenciais, repositórios e informações do agente.
- **Gerenciar proteção.** Proteja máquinas usando o AppAssure Agent e gerencie sua proteção.
- **Gerenciar replicação.** Comece a replicar os agentes a partir de um core de origem para um core de destino para a preparação de recuperação após desastres.
- **Monitorar.** Visualize as máquinas e os eventos que o Core ou os Cores realizam.
- **Relatórios.** Criar, visualizar e enviar relatórios de informações e eventos da máquina.

Gerenciamento de credenciais do AppAssure Core e do agente

O AppAssure Core fornece os serviços essenciais de cópia de segurança, replicação, arquivamento e gerenciamento. Um agente é uma máquina com o AppAssure Agent instalado que é gerenciada e protegida por um core específico. Em um servidor core, repositórios são definidos para armazenar os snapshots que são capturados nas máquinas protegidas, isto é, nos AppAssure Agents. Os repositórios são configurados especificando em quais volumes no servidor do Core os dados serão armazenados.

Gerenciamento das credenciais do agente

Quando um core protege um agente em um domínio de rede diferente, você precisa configurar as credenciais de rede para permitir que o Core se comunique com o agente.

Para gerenciar as credenciais do agente

1 Navegue até a seção Configurar gerenciamento e selecione **Gerenciar credenciais do Agent**.

2 Insira as seguintes informações da sua máquina AppAssure Agent e clique em **Aplicar**.

Tabela 6.

Caixa de texto	Descrição
Login	Insira o nome de usuário para se conectar à máquina. Por exemplo: administrador.
Senha	Insira a senha associada ao login.
Confirmar senha	Insira novamente a senha associada ao login.
Domínio	Insira o domínio desta máquina, caso aplicável. Se a máquina não estiver em um domínio, deixe essa caixa de texto vazia.

3 Selecione uma máquina e clique em **Confirmar** para confirmar se as credenciais salvas estão corretas e se têm os privilégios necessários para comunicarem-se com agente.

Gerenciamento das credenciais do Core

Quando um AppAssure Core protege agentes em um grupo de trabalho ou domínio de rede diferente, você precisa configurar as credenciais de rede para permitir que o Core se comunique com o agente.

Para gerenciar as credenciais do core

1 Navegue até a seção Configurar gerenciamento e selecione **Gerenciar credenciais do Core**.

2 Insira as seguintes informações da sua máquina AppAssure Core e clique em **Aplicar**.

Tabela 7.

Caixa de texto	Descrição
Login	Insira o nome de usuário para se conectar à máquina. Por exemplo: administrador.
Senha	Insira a senha associada ao login.
Confirmar senha	Insira novamente a senha associada ao login.
Domínio	Insira o domínio desta máquina, caso aplicável. Se a máquina não estiver em um domínio, deixe essa caixa de texto vazia.

3 Selecione uma máquina e clique em **Confirmar** para confirmar se as credenciais salvas estão corretas e se fornecem os privilégios necessários para comunicar-se com o Core.

Configuração de repositórios

Os repositórios são usados para armazenar os snapshots capturados nos servidores protegidos. Antes de criar um repositório, confirme que você configurou as credenciais usadas para efetuar login no AppAssure Core associado.

NOTA: Os repositórios do AppAssure devem ser armazenados em dispositivos de armazenamento primários. Dispositivos de armazenamento de arquivamento como Domínio de dados não são suportados devido a limitações de desempenho. De forma semelhante, os repositórios não devem ser armazenados em arquivadores NAS organizados em níveis na nuvem, pois esses dispositivos tendem a ter limitações de desempenho quando usados como armazenamento primário.

Adição de um repositório

Execute as etapas deste procedimento para adicionar um repositório

Para adicionar um repositório

1. Navegue até a seção Configurar gerenciamento e selecione **Gerenciar repositórios do Core**.
2. Na lista de máquinas nesta página, selecione a máquina Core na qual você deseja adicionar um repositório.
3. Clique em **Adicionar novo repositório**.

   A caixa de diálogo Adicionar novo repositório é exibida.
4. Insira as informações nas caixas de texto conforme descrito na tabela a seguir.

   Tabela 8.

Caixa de texto	Descrição
Nome	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número de índice, que corresponde ao número do novo repositório. Você pode alterar o nome conforme necessário, inserindo até 150 caracteres.
Operações simultâneas	Defina o número de solicitações simultâneas suportadas pelo repositório. Por padrão, o valor é 64.
Comentários	(opcional) Ao configurar os repositórios, os locais de armazenamento local e de rede precisam ser semelhantes e não uma combinação de locais de arquivos locais e de rede. Configure o local de armazenamento dos repositórios como *todos locais* ou *todos em rede*. Insira uma nota descritiva sobre este repositório.

5. Clique em **Adicionar especificação do arquivo** para definir um volume ou local de armazenamento específico para o repositório.

AVISO: Se o repositório do AppAssure que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você não definir uma pasta dedicada para armazenar os arquivos do repositório, esses arquivos serão armazenados na raiz. Excluir o repositório também exclui todos os conteúdos da raiz, resultando em perda de dados catastrófica.

NOTA: Os repositórios do AppAssure devem ser armazenados em dispositivos de armazenamento primários. Dispositivos de armazenamento de arquivamento como Domínio de dados não são suportados devido a limitações de desempenho. De forma semelhante, os repositórios não devem ser armazenados em arquivadores NAS organizados em níveis na nuvem, pois esses dispositivos tendem a ter limitações de desempenho quando usados como armazenamento primário.

A caixa de diálogo Adicionar especificação de arquivo é exibida.

6 Especifique onde e como adicionar o arquivo ao local de armazenamento. Você pode selecionar adicionar o arquivo no disco local ou no compartilhamento de CIFS.

NOTA: Ao configurar os repositórios, você não pode misturar localizações locais e de rede para um determinado repositório. O local de armazenamento precisa ter todos os arquivos locais ou todos os arquivos em rede.

- Clique em **Adicionar arquivo no disco local** para especificar uma máquina local e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 9.

Caixa de texto	Descrição
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite: `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Caminho de dados	Insira o local para armazenar os dados protegidos. Por exemplo, digite: `X:\Repository\Data`. As mesmas limitações do caminho se aplicam; use somente caracteres alfanuméricos, hífen ou ponto, sem espaços ou caracteres especiais.

- Ou clique em **Adicionar arquivo no compartilhamento de CIFS** para especificar um local de compartilhamento de rede e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 10.

Caixa de texto	Descrição
Caminho de UNC	Insira o caminho para o local de compartilhamento de rede. Se esse local estiver na raiz, defina um nome de pasta dedicada (por exemplo, `Repository`). O caminho precisa começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento de rede.
Senha	Especifique a senha para acessar o local de compartilhamento de rede.
Confirmar senha	Reinsira a senha.

7 No painel Detalhes, insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 11.

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é *512*.
Média de bytes por registro	Especifique a média de bytes por registro. O valor padrão é *8192*.

Tabela 11.

Caixa de texto	Descrição
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como *Ligado*, que é o padrão, o Windows controla o armazenamento em cache. **NOTA:** Definir a política de cache de gravação como *Ligado* pode resultar em desempenho mais rápido. Se você estiver usando uma versão do Windows Server anterior à Server 2012, a definição recomendada é *Desligado*. Se definido como *Desligado*, o AppAssure controla o armazenamento em cache. Se definido como *Sincronizar*, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.
Tamanho	Defina o tamanho ou capacidade do local de armazenamento. O padrão é 250MB. Você pode selecionar dentre os seguintes: • MB • GB • TB **NOTA:** O tamanho que você especificar não pode exceder o tamanho do volume. Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16TB. Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo será de 256 TB. **NOTA:** Para que o AppAssure valide o sistema operacional, o Windows Management Instrumentation (WMI) deve ser instalado no local de armazenamento pretendido.

8 Clique em **Salvar**.

A página Repositórios exibe o local de armazenamento recém-adicionado.

9 Repita da Etapa 5 à Etapa 8 para adicionar outros locais de armazenamento ao repositório.

10 Clique em **Criar** para criar o repositório.

- Se for necessário editar o local de armazenamento, clique em **Editar**.
- Se for necessário excluir o local de armazenamento, clique em **Excluir**.

Realização de uma auditoria de repositório

Realizar uma auditoria de repositório é útil para obter e visualizar informações sobre os repositórios configurados para um AppAssure Core.

Para realizar uma auditoria de repositório

1 Navegue até a seção Configurar gerenciamento e selecione **Gerenciar repositórios do Core**.

2 Selecione a máquina na qual você deseja realizar a auditoria e clique em **Obter repositórios do AppAssure Core**.

3 Para confirmar a seleção e reconhecer que essa tarefa consulta todos os cores gerenciados quanto a seus parâmetros de repositório, clique em **Sim**.

Todos os repositórios associados, incluindo o tamanho alocado (em MB, GB ou TB) serão exibidos na coluna Repositórios da máquina selecionada.

Visualização de informações do volume do AppAssure Agent

Você pode facilmente visualizar informações sobre os volumes sendo protegidos em máquinas AppAssure Agent. Para obter informações atualizadas sobre o volume do AppAssure Agent, certifique-se de que você definiu as credenciais usadas para efetuar login na máquina do agente.

Para visualizar informações do volume do AppAssure Agent

1 Navegue até a seção Configurar gerenciamento e clique em **Informações dos volumes Agent**.

2 Para atualizar as informações na lista dos volumes conhecidos do AppAssure Agent, clique em **Obter volumes do AppAssure Agent**.

3 Na caixa de diálogo de confirmação, clique em **Sim**.

Configuração da proteção de máquina

Você pode proteger os volumes de dados nas máquinas e nos servidores Windows nos quais você instalou os AppAssure Agents. Quando uma máquina é protegida, snapshots completos e incrementais dos dados são capturados e armazenados no repositório do core associado.

Esta seção inclui os seguintes tópicos:

- Proteção de uma máquina
- Atualização do status de proteção e replicação
- Remoção de uma máquina da proteção

Proteção de uma máquina

Antes de proteger uma máquina, certifique-se de ter informações disponíveis para os volumes do agente e os repositórios do core.

Para proteger uma máquina

1 Navegue até a seção Gerenciar proteção e clique em **Proteger máquinas**.

2 Na lista de máquinas nesta página, selecione a máquina que você deseja proteger.

3 Clique em **Proteger Agent**.

A caixa de diálogo Proteger máquina é aberta.

4 Na guia Selecionar Core, selecione o Core que protege e gerencia esta máquina do agente e clique em **Avançar**.

5 Na guia Opções, selecione os volumes a serem protegidos no agente e os repositórios do Core nos quais os snapshots do volume serão armazenados e, a seguir, clique em **Proteger**.

Uma mensagem será exibida na coluna Gerenciado por Core, indicando que a configuração da proteção está em andamento. Após a configuração, o nome do Core será exibido nesta coluna. O intervalo padrão de proteção é de uma hora.

Atualização do status de proteção e replicação

Ao atualizar o status de proteção e replicação de uma máquina, você obtém o status mais recente de todos os agentes associados aos cores conhecidos. Esse recurso é útil caso você precise garantir que tem a versão mais recente dos dados protegidos.

Para atualizar o status de proteção e replicação

1. Navegue até a seção Gerenciar proteção e clique em **Proteger máquinas**.
2. Clique em **Atualização do status de proteção e replicação**.
3. Na caixa de diálogo de confirmação, clique em **OK**.

Remoção de uma máquina da proteção

Ao remover uma máquina da proteção, você interrompe a proteção fornecida pelo AppAssure Core ao qual o AppAssure Agent (na máquina em questão) está vinculado.

NOTA: A máquina é simplesmente removida da proteção, mas o software AppAssure Agent continua instalado.

Para remover uma máquina da proteção

1. Navegue até a seção Gerenciar proteção e clique em **Proteger máquinas**.

   Na lista de máquinas nesta página, encontre a máquina que você deseja remover e, na coluna Ações, clique em **Remover máquina**.

   A caixa de diálogo Remover máquina é aberta.
2. Confirme as credenciais da máquina, caso necessário.
3. Para remover os pontos de recuperação da máquina, selecione **Excluir pontos de recuperação**.
4. Clique em **Remover máquina**.

   Uma mensagem é exibida na coluna Gerenciado por Core da máquina selecionada indicando que a remoção está em andamento.

Gerenciamento da replicação

A replicação é o gerenciamento e a transferência de dados (pontos de recuperação) entre um core de origem e de destino. Um snapshot dos pontos de recuperação no core de origem é capturado e transmitido para um core de destino para redundância. Há diversas maneiras de configurar a replicação, por exemplo, entre dois cores no mesmo site ou entre dois locais por máquina. O AppAssure transmite de maneira assíncrona o snapshot dos dados replicados (pontos de recuperação) ao core de destino para armazenamento. A replicação de saída também pode ser configurada para um provedor de serviço gerenciado (MSP), fornecendo serviços de recuperação após desastres e cópia de segurança fora do local ou para um core autogerenciado.

O AppAssure Add-on for Kaseya suporta dois tipos de replicação. A replicação por solicitação é útil quando você sabe o nome, porém não sabe as credenciais do Core no qual deseja fazer a replicação. Por exemplo, um core hospedado por MSP. Já a replicação por demanda é a replicação de um core autogerenciado, isto é, um core de sua propriedade.

No AppAssure Add-on for Kaseya, a seguinte lista descreve as tarefas de replicação que você pode realizar:

- Ao se preparar para a replicação, você cria um vínculo entre dois cores, isto é, um core de origem e um de destino. Para obter mais informações, consulte Preparação para replicação.
- Ao estabelecer a replicação, você inicia uma replicação sob demanda para todas as replicações preparadas. Para obter mais informações, consulte Estabelecimento da replicação.

- Ao visualizar solicitações pendentes, você pode aceitar ou recusar solicitações de replicação. Para obter mais informações, consulte Visualização de solicitações de replicação pendentes.
- Também é possível remover a replicação. Para obter mais informações, consulte Remoção da replicação.

Preparação para replicação

Use a tarefa Preparar replicação para configurar a replicação e criar um vínculo entre dois cores, isto é, um core de origem e um de destino.

Para se preparar para replicação

1 Navegue até a seção Gerenciamento da replicação e clique em **Preparar replicação**.

2 Na lista de máquinas nesta página, selecione a máquina que você deseja preparar para replicação e clique em **Preparar replicação**.

A caixa de diálogo Preparar replicação será aberta.

3 Na guia Selecionar tipo de replicação, efetue um dos seguintes procedimentos:

- Para efetuar uma replicação por solicitação, selecione a opção **Eu possuo uma assinatura com um terceiro que oferece cópia de segurança em outro local e serviços de recuperação após desastres e desejo replicar minhas cópias de segurança nesse serviço (gerar solicitação de replicação)**, e depois insira as informações descritas na tabela a seguir.

Tabela 12.

Caixa de texto	Descrição
Nome do host	Insira o nome de domínio totalmente qualificado (FQDN) para o Core.
Porta	Insira o número da porta recebido do provedor de serviços. O número de porta padrão é 8006.

- Para uma replicação sob demanda, selecione a opção **Eu possuo meu próprio core remoto no qual desejo realizar a replicação (estabelecer replicação sob demanda)** e insira as seguintes credenciais para o core de destino como são descritas na tabela a seguir.

Tabela 13.

Caixa de texto	Descrição
Nome do host	Insira o nome de host para o Core.
Porta	Insira o número da porta. O número de porta padrão é 8006.
Nome de usuário	O nome de usuário usado para efetuar login no Core.
Senha	A senha associada a esse nome de usuário.

4 Clique em **Continuar**.

5 Se você selecionou a opção de replicação por solicitação, na guia Adicionar core remoto, faça o seguinte:

a Selecione a máquina AppAssure Agent para replicação.

b Insira o endereço de e-mail de assinatura e o ID do cliente (opcional) recebido pelo provedor do serviço.

c Clique em **Enviar solicitação** para fechar a caixa de diálogo e enviar a solicitação de replicação.

Na página Preparar replicação, uma mensagem será exibida na coluna Estado indicando que a replicação por solicitação está em andamento, seguido por um status de *Pendente*. Se a solicitação for aprovada, o status mudará para *Estabelecido*. No caso de replicação sob demanda, a coluna Estado exibirá o texto *Emparelhamento*.

6 Se você selecionou o opção de replicação sob demanda, vá para a seção Estabelecimento da replicação.

Estabelecimento da replicação

Use Estabelecer replicação para configurar a replicação sob demanda quando tiver credenciais para cores de origem e de destino. Por exemplo, você possui os Cores e não precisa enviar uma solicitação ou obter aprovação para estabelecer replicação.

Para estabelecer a replicação

1. Navegue até a seção Gerenciamento da replicação e clique em **Estabelecer replicação**.
2. Na lista de máquinas nesta página, selecione a máquina que foi preparada para replicação e com a qual você deseja estabelecer a replicação. (Essa máquina apresenta o status *Preparação de replicação validada* na coluna Estado.)
3. Clique em **Estabelecer replicação**.

   A caixa de diálogo Estabelecer replicação será aberta.
4. Em Adicionar Core remoto, faça uma destas ações:
   - Selecione **Substituir um Core replicado existente em** e selecione um core de destino existente na lista suspensa.
   - Selecione **Criar um novo core replicado em** e insira o nome do novo core de destino.
5. Na tabela, selecione a(s) máquina(s) do agente e um repositório no qual deseje armazenar os dados replicados a partir de uma lista suspensa para cada máquina.
6. Clique em **Iniciar replicação**.

   Na página Estabelecer replicação, a coluna Estado da máquina de core selecionada exibe o texto *Pendente*. Quando a replicação for estabelecida, o status é alterado para *Estabelecido*.

Visualização de solicitações de replicação pendentes

Se você tiver máquinas do agente para as quais outras podem enviar solicitações de replicação, esta página permitirá que você obtenha e visualize as solicitações enviadas a essas máquinas. A lista de agentes inclui as seguintes informações:

- **Nome do Core.** O nome da máquina que possui o Core instalado.
- **Credenciais.** O nome de usuário associado à máquina.
- **Selecionar.** Os meios pelos quais você pode selecionar uma máquina.
- **ID do cliente.** O número de identificação do cliente que fez a solicitação de replicação.
- **Endereço de e-mail.** As informações de contato para o cliente que solicitou a replicação para esse core.
- **Nome do host.** O nome do core de origem a partir do qual o cliente deseja replicar.
- **Status.** O estado de replicação entre os cores (por exemplo, Pendente ou Aprovado).

Você pode então revisar essas solicitações e aceitá-las ou recusá-las conforme apropriado. Ao aceitar uma solicitação, a replicação é estabelecida e os pontos de recuperação são enviados dos cores de origem para os de destino.

Para visualizar solicitações de replicação pendentes

1. Navegue até a seção Gerenciamento da replicação e clique em **Solicitações pendentes**.
2. Na página Solicitações pendentes, na coluna Selecionar, selecione uma máquina da lista com o status Pendente.
3. Para atualizar a lista, clique em **Obter solicitações pendentes** e depois clique em **Sim** na caixa de diálogo para confirmar.
4. Selecione o Core novamente e clique em **Revisar**.

   A caixa de diálogo Solicitação pendente será aberta.

5 Se desejar aprovar a solicitação, em Revisar solicitações de replicação, faça o seguinte:

   a Selecione a máquina de destino para a qual você deseja efetuar a replicação ou insira um novo core remoto para a replicação inserindo as seguintes informações:

      - Nome do Core
      - Endereço de e-mail de assinatura
      - (Opcional) ID do cliente para essa máquina

   b Selecione as máquinas do agente e os repositórios associados para a replicação.

   c Como opção, insira um comentário para o cliente ver.

   d Clique em **Enviar resposta** para estabelecer a replicação.

6 Para recusar a solicitação, clique em **Recusar**.

   Na página Solicitações pendentes, a coluna Status será atualizada para exibir o status como *Aprovado* ou *Recusado*, conforme apropriado.

Remoção da replicação

Ao remover uma replicação, você interromperá qualquer tipo de replicação do agente. Depois de remover a replicação no console do add-on, o emparelhamento entre o core de origem e o core de destino continuará existindo. Para remover a replicação por completo, é preciso usar o Core Console em cada máquina. Para obter mais informações sobre a remoção da replicação do aplicativo do AppAssure Core Console, consulte o *Guia do usuário do Dell AppAssure*.

Para remover a replicação

1 Navegue até a seção Gerenciamento da replicação e clique em **Remover replicação**.

2 Selecione a máquina do agente para a qual deseja remover a replicação e depois clique em **Remover replicação**.

   DICA: Para selecionar todas as máquinas, clique em **Selecionar todos** na primeira coluna da tabela.

   A caixa de diálogo Remover replicação será aberta.

3 Para remover também os pontos de recuperação associados, clique em **Excluir pontos de recuperação**.

4 Clique em **Remover**.

Monitoramento da atividade do AppAssure

No AppAssure Add-on for Kaseya, você pode visualizar informações pertinentes sobre a atividade de todas as máquinas no seu ambiente AppAssure for Kaseya. Detalhes, incluindo nome da máquina, endereço IP, versão do software AppAssure e tipo de máquina (core ou agente), identificam cada máquina.

Para monitorar a atividade do AppAssure

1 Navegue até a seção Monitorar e clique em **Máquinas**.

2 Na coluna Ações de uma máquina específica, clique no link **Tarefas** para visualizar uma lista com todas as tarefas associadas a uma máquina específica.

   Na página Tarefas, você pode visualizar informações como o tipo de tarefa, quando ela foi iniciada, se foi ou não concluída e seu status.

3 Clique em **Atualizar** para atualizar a lista de tarefas.

4 Para ver detalhes sobre uma tarefa específica, clique em **Visualizar resultado** para essa tarefa.

Gerenciamento de relatórios do AppAssure Core

O AppAssure Add-on for Kaseya permite gerar relatórios para um ou mais cores. Ele não gera relatórios para agentes individuais. No entanto, os relatórios incluem informações sobre os agentes que os cores selecionados protegem.

Com o add-on, é possível gerar os seguintes relatórios:

- Relatório resumido do Core
- Relatório de evento crítico

O relatório resumido do core fornece detalhes sobre trabalhos realizados e o status desses trabalhos. Também gera um relatório de status do core. Juntos, os relatórios incluem as seguintes informações:

- **Nome do Core.** O nome do Core selecionado para o relatório.
- **Status dos dados.** O status dos dados que o Core incluiu na cópia de segurança (por exemplo, Disponível).
- **Core.** O Core para o qual você executou o relatório.
- **Máquina.** O nome do agente que o Core protege.
- **Tipo.** O tipo de trabalho realizado (por exemplo, Transferência).
- **Resumo.** Uma breve descrição das ações que o trabalho realizou.
- **Status.** O status do trabalho (por exemplo, Bem-sucedido ou Com falha).
- **Erro.** O tipo de erro que causou a falha, caso tenha ocorrido uma falha.
- **Hora inicial.** A hora em que o trabalho iniciou.
- **Hora de término.** A hora em que o trabalho terminou.
- **Tempo.** A duração do trabalho (por exemplo, 2m 16s para 2 minutos e 16 segundos).
- **Trabalho total.** A quantidade de dados afetados. Por exemplo, um trabalho de transferência poderia ter um trabalho total de 53,7 MB.

O relatório de evento crítico também gera um relatório de status do core. Juntos, os relatórios incluem as seguintes informações:

- **Nome do Core.** O nome do Core selecionado para o relatório.
- **Status dos dados.** O status dos dados que o Core incluiu na cópia de segurança (por exemplo, Disponível).
- **Core.** O Core para o qual você executou o relatório.
- **Nº de falhas.** O número de trabalhos que não puderam ser concluídos no Core selecionado.

Os seguintes procedimentos descrevem como criar e visualizar relatórios.

Criação de relatórios

O AppAssure Add-on for Kaseya fornece um recurso de relatórios consolidados que permite criar relatórios de resumo para os AppAssure Cores selecionados e atividades para os AppAssure Agents protegidos pelo Core.

Para criar relatórios

1 Navegue até a seção Relatórios e clique em **Criar relatório**.

2 Selecione os Cores para os quais você deseja criar o relatório.

> **DICA:** Para selecionar todas as máquinas de core na tabela, clique em **Selecionar todos** na primeira coluna da tabela.

3 (opcional) Na caixa de texto Descrição, insira uma descrição em texto.

4 No calendário suspenso de hora inicial, selecione uma data e então insira um horário em que o relatório deve começar.

5 No calendário suspenso de hora de término, selecione uma data e então insira um horário em que o relatório deve terminar.

6 Clique em **Executar relatório**.

7 Na caixa de diálogo, clique em **OK** para confirmar que o relatório foi programado.

Na coluna Status do relatório mais recente, o status Em progresso será exibido. O status será alterado para Concluído quando o relatório for criado.

8 Para visualizar o relatório, execute as etapas na seção a seguir, Visualização de relatórios.

Visualização de relatórios

Depois de criar relatórios resumidos para o AppAssure Add-on for Kaseya, é possível visualizá-los. Os relatórios são úteis para a conformidade e contêm informações sobre as atividades do AppAssure Core e do AppAssure Agent associadas ao Core.

Execute as etapas do procedimento a seguir para visualizar os relatórios de resumo. Para obter mais informações sobre como criar os relatórios, consulte Criação de relatórios.

Para visualizar os relatórios

1 Navegue até a seção Relatórios e clique em **Visualizar relatórios**.

2 Na coluna Ações para o nome dos relatórios gerados, clique no link para o relatório que deseja visualizar (por exemplo, Visualizar relatório resumido do Core).

A página Visualizar relatórios será atualizada e exibirá todos os detalhes do relatório.

Em Relatório de status do Core, você pode visualizar o status do Core no relatório (por exemplo: Disponível).

Em Relatório resumido do Core, você pode visualizar uma lista detalhada com as atividades do agente associado ao Core no relatório. Esses detalhes incluem o tipo de atividade, uma descrição resumida, o status, o horário inicial e de término, a duração da atividade e a quantidade de espaço em disco necessária para a atividade.

3 Se o relatório ocupar diversas páginas, você pode clicar nos números de página ou nos botões de seta na parte inferior dos resultados do relatório para mudar de página.

4 Para exportar os resultados do relatório em um formato diferente, selecione o formato da exportação na lista suspensa e clique em **Salvar**.

- Os formatos disponíveis incluem PDF, XLS, XLSX, CSV e HTML.

5 Para imprimir os resultados do relatório, use uma das seguintes opções:

- Clique no primeiro ícone de Impressora para imprimir todo o relatório.
- Ou clique no segundo ícone de impressora para imprimir a página atual do relatório.

Sobre a Dell

A Dell escuta os clientes e fornece tecnologia inovadora, soluções empresariais e serviços globais de confiança e valor. Para obter mais informações, visite www.software.dell.com.

Contatos da Dell

Suporte técnico:
Suporte online

Vendas e dúvidas sobre produtos:
(800) 306-9329

E-mail:
info@software.dell.com

Recursos do suporte técnico

O suporte técnico está disponível para clientes que compraram produtos de software da Dell com um contrato de manutenção válido e clientes que estão usando versões de teste. Para acessar o Portal de suporte, visite http://software.dell.com/support/.

O Portal de suporte fornece ferramentas de autoajuda, que você pode usar para resolver problemas de forma rápida e independente, 24 horas por dia, 365 dias por ano. Além disso, o Portal fornece acesso direto a engenheiros de suporte de produtos por meio de um sistema online de Solicitação de serviço.

O site permite que você:

- Crie, atualize e gerencie as Solicitações (casos) de serviço.
- Visualize artigos da Base de conhecimento.
- Obtenha notificações de produtos.
- Baixe o software. No caso de software de teste, acesse Downloads de teste.
- Assista a vídeos instrucionais.
- Participe de discussões da comunidade.
- Converse com um engenheiro do suporte.